ICS 33.050
M 30

团　体　标　准

T/TAF 071.1-2020

智能家居终端设备 通用安全能力技术要求

Smart home terminal equipment
Common technical requirements for security capability

2020-09-14 发布　　2020-09-14 实施

电信终端产业协会　发布

目　　次

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准中的某些内容可能涉及专利。本标准的发布机构不承担识别这些专利的责任。

本标准由电信终端产业协会提出并归口。

本标准起草单位：中国信息通信研究院、青岛海尔通信有限公司、小米通讯技术有限公司、中国电信移动终端运营中心、OPPO广东移动通信有限公司、百度在线网络技术（北京）有限公司、中国联合网络通信有限公司、北京奇虎科技有限公司、联想（北京）有限公司。

本标准起草人：宁华、刘陶、吴怡、周飞、傅山、王艳红、杜云、王淼、祖岩岩、井皓、周圣炎、江小威、李腾、吴月升、姚一楠。

引　言

随着物联网、大数据分析等技术的深入应用，我国智能家居产业近年来得到快速发展，智能安防、智能计量、智能门锁、智能家电等智能家居应用给用户日常生活带来极大便利。与此同时，作为与消费者生活紧密相关的消费领域，智能家居所面临的安全威胁也日趋凸显，针对智能家居终端设备的恶意攻击种类不断更新，用户隐私信息泄露、中间人攻击、恶意远程操控等事件反复曝光，给用户信息、财产和人身安全带来极大困扰。智能家居设备的信息安全问题已成为制约产业发展的重要因素之一。为提高智能家居终端设备自身的安全防护能力，指导相关厂商规范设计开发智能家居终端产品，同时为安全性测试评估提供参考依据，特制定本标准。本标准是基于智能家居终端设备所面临的安全威胁和通用安全需求，结合国内外相关安全技术和相关标准研究编制。

本标准主要对智能家居终端设备的安全防护提出通用技术要求，强化保护力度，完善保护体系，以防范各类安全威胁，避免用户的利益受到损害。

智能家居终端设备 通用安全能力技术要求

1 范围

本标准规定了智能家居的终端设备通用安全能力的技术要求，包括智能家居硬件安全能力、智能家居操作系统安全能力、智能家居外围接口安全能力、智能家居应用层安全能力、智能家居无线通信安全能力、智能家居用户数据保护安全能力、智能家居终端能耗安全保护能力等。

本标准适用于智能家居终端设备，个别条款不适用于特殊行业、专业应用，其他类似设备也可参考使用。

2 规范性引用文件

下列文件对于本标准的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本标准。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

YD/T2407-2013 移动智能终端安全能力技术要求

3 术语、定义和缩略语

3.1 术语和定义

3.1.1

智能家居终端 smart home terminal

智能家居终端是连接到家庭网络的、协同提供智能家居服务的各种终端设备，包括：智能家居网关设备、控制设备、以及提供安防、测量、控制、娱乐等服务的相关应用设备。

3.1.2

智能家居网关设备 smart home gateway device

同时与公共通信网络、智能家居控制设备和应用终端相连的设备，为应用设备分配通讯地址，根据分配的通讯地址与智能家居应用设备通信，并完成控制设备与应用设备之间的信令转换，将转换后的信令发送至智能家居控制设备或应用设备。

3.1.3

智能家居控制设备 smart home controller device

根据接收的用户指令或预先配置的任务，执行智能家居控制逻辑，通过智能家居网关向智能家居应用设备发出指令，通过智能家居应用设备对指令的执行，实现智能家居应用。常见控制模式包括，场景控制、组合控制、关联控制、远程控制等。

3.1.4

智能家居应用设备smart home application device

与智能家居网关设备相连，通过对接收指令的执行，实现智能家居应用的设备。智能家居应用设备常见使用场景如附录A所示。

4 智能家居终端设备安全能力框架及目标

4.1 主要安全风险

智能家居终端安全涉网关设备、控制设备、应用设备三类设备，各部分典型业务流程如下图1所示。

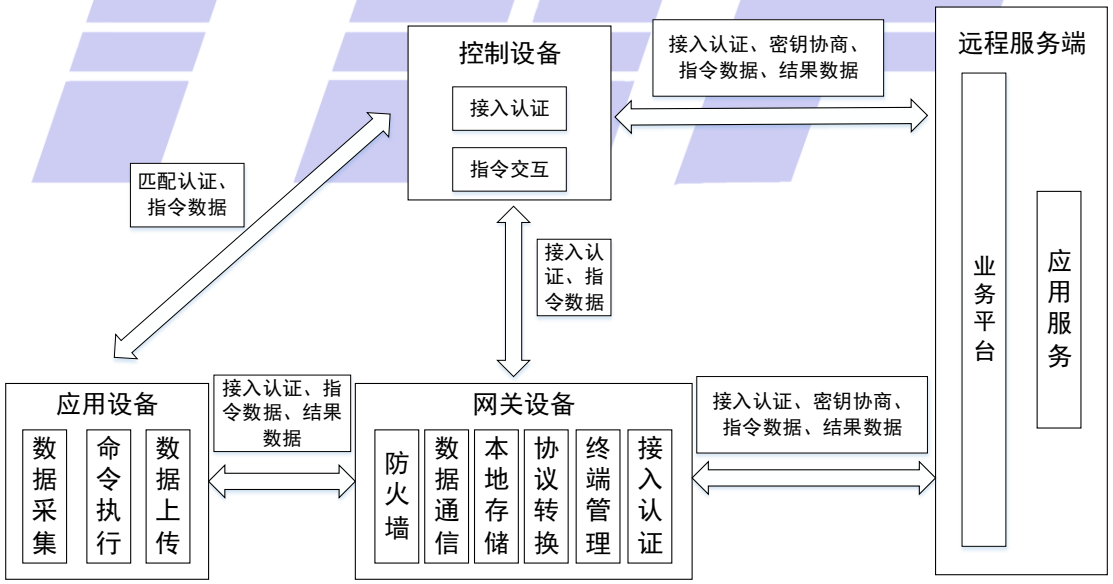

图 1 智能家居终端应用流程

智能家居终端设备的安全风险存在于硬件、操作系统、应用软件、外围接口、通信、用户数据、能耗七个方面。各层次所面临的主要风险见表1。

表 1 智能家居终端设备重要安全风险

对象	主要安全风险
硬件	（1）非授权的访问； （2）功能失效、设备不可用； （3）假冒设备；
操作系统	（1）非授权的访问； （2）审计数据丢失； （3）恶意代码攻击
应用软件	（1）非授权访问； （2）软件漏洞； （3）恶意代码攻击；
外围接口	（1）非授权访问； （2）审计失效；
通信	（1）通信数据泄露、篡改、丢失； （2）传输中断、拦截、篡改、伪造； （3）拒绝服务攻击，重放攻击，中间人攻击； （4）虚假路由； （5）通信协议漏洞
用户数据	（1）用户数据泄露
能耗	（1）能耗攻击，设备失效

4.2 安全能力框架

图2为智能家居终端设备安全能力框架图，主要包括7个部分，最底层是智能家居终端设备硬件安全能力，之上为操作系统安全能力，再上为应用层安全能力和外围接口安全能力，最顶层为无线通信安全能力，能耗保护安全能力及用户数据保护安全能力涉及以上各个层面。

图 2 智能家居终端设备安全能力框架图

4.3 安全目标

4.3.1 智能家居硬件安全目标

智能家居硬件安全目标是在芯片级保证设备存储及处理芯片安全，避免芯片内的操作系统、数据、程序等被非法获取或者篡改。

4.3.2 智能家居操作系统安全目标

操作系统安全目标是达到操作系统对系统资源调用的监控、保护、提醒，确保涉及安全的系统行为总是在受控的状态下，不会出现用户在不知情情况下某种行为的执行，或者用户不可控的行为的执行。另外操作系统还应保证自身的升级是受控的。

4.3.3 智能家居外围接口安全目标

外围接口安全目标是要保证智能家居网关的web、ssh、telnet、console等外围接口应具有必要的安全防护措施，防止攻击者通过外围接口入侵并控制网关设备。

4.3.4 智能家居应用层安全目标

应用层安全目标是要保证智能家居终端设备对要安装在其上的应用软件可进行来源的识别，对已经安装在其上的应用软件可以进行敏感行为的控制。另外还要确保预置在智能家居设备中的应用软件无损害用户利益和危害网络安全的行为，例如：未经授权敏感信息采集、越权数据操作、向外传送用户数据等行为。

4.3.5 智能家居无线通信安全目标

无线通信安全目标是要保证智能家居终端设备采用Wifi或者Zigbee、蓝牙等无线协议在网内传输的数据应采用必要数据加密和完整性校验等手段进行安全防护，且加密算法强度应满足国家相关规范，防止认证、标识、口令、隐私等敏感数据在无线传输过程中被获取甚至篡改。同时，网关设备端无线热点应具有相应的身份鉴别能力，避免非授权的终端设备接入。

4.3.6 智能家居用户数据保护安全目标

用户数据保护安全目标是要保证用户数据的安全存储，确保用户数据不被非法访问、不被非法获取、不被非法篡改，同时能够通过备份保证用户数据的可靠恢复。

4.3.7 智能家居终端设备能耗保护安全目标

终端设备能耗保护安全目标是要保证终端电池的正常、稳定消耗，避免由于外部的蓄意攻击而导致电池非预期耗尽。

5 安全能力技术要求

5.1 基本配置要求

5.1.1 智能家居网关设备基本配置要求

智能家居网关设备基本配置要求如下：

a) 与智能家居应用设备捆绑使用，承载应用设备接入控制功能的网关设备，应支持所连接应用设备的注册和管理；
b) 与智能家居应用设备捆绑使用，承载应用设备接入控制功能的网关设备，应支持所连接应用设备运行状态收集上报，如设备标识、位置信息、固件版本、系统版本、网络类型、用户信息等；
c) 与智能家居应用设备捆绑使用，承载应用设备接入控制功能的网关设备，应支持对接入的应用设备，实现软件升级、固件更新、远程维护及配置管理等功能；
d) 与智能家居应用设备捆绑使用，承载应用设备接入控制功能的网关设备，应支持对接入的应用设备，实现故障管理、性能管理、配置管理等功能；
e) 与智能家居应用设备捆绑使用，承载应用设备接入控制功能的网关设备，应支持对接入的应用设备进行注销、禁用和锁定管理，当接入设备丢失时，登录、访问等敏感数据应被自动擦除，防止恶意利用。

5.1.2 智能家居控制设备基本配置要求

智能家居控制设备基本配置要求如下：

a) 应支持与服务端之间的通信认证和密钥协商功能；

b) 应支持与智能家居网关之间的接入认证功能；
c) 使用移动智能终端作为智能家居控制设备的，应符合 YD/T 2407-2013 《移动终端安全能力要求》标准一级要求。

5.1.3 智能家居应用设备基本配置要求

应支持与智能家居网关之间的接入认证功能。

5.2 硬件安全能力

5.2.1 硬件功能安全

硬件电路功能实现应与提供给用户的设计文档相一致，不应存在未声明或隐藏的功能。例如应关闭隐藏调试功能，防止厂商在未获得用户授权的情况下获得对芯片内存的访问或芯片功能更改的能力。

5.2.2 硬件设计安全

硬件设计安全要求包括但不限于：

a) 硬件内部模块的安全属性和芯片间通信协议等安全敏感实现应不存在设计原理上的缺陷，例如由于随机数的随机性较差而导致的弱密钥等；
b) 密码算法的安全性应符合相关国家和行业标准要求，密钥的产生、分发、使用、存储、销毁应有相应安全保障机制；
c) 应关闭不必要的下载、调试端口。

5.2.3 硬件容错能力

应具备容错能力，能够防御由针对芯片的差分错误、故障代数等故障注入攻击所导致的功能失效。

5.2.4 芯片安全能力

芯片安全能力要求包括但不限于：

a) 对于支持安全模块的芯片，应具备固件芯片的物理写保护的功能，防止固件被篡改；
b) 对于支持安全模块的芯片，宜具备侧信道攻击防护能力；
c) 宜具备安全启动硬件保护能力；
d) 宜具备安全域隔离功能，提供可信执行环境；
e) 芯片宜使用拆卸存迹硬质涂层，防止直接观察、探测芯片内容，并在企图拆卸或移动芯片后留下证据；
f) 应开启芯片的读保护功能，防止固件被读取后进行逆向、篡改。

5.3 操作系统安全能力

5.3.1 安全启动

在启动过程中，所有启动程序（例如引导程序、内核镜像、基带固件等）必须通过完整性校验才可以加载运行，防止加载并运行未经授权的恶意程序。

5.3.2 设备接入控制能力

设备接入控制能力要求包括但不限于：

a) 智能家居终端设备应具备身份鉴别和接入认证能力。避免由于非法设备的接入，而导致的敏感数据泄露、功能异常或失效；
b) 设备所使用的密码算法应符合国家法律法规和行业主管部门的规定和技术标准；
c) 如存在密钥协商过程，应基于非对称密码算法进行密钥协商，通信数据应进行加密；
d) 智能家居网关设备应具备带宽控制功能，防止选择性转发、洪泛攻击等所导致的应用设备失效或可用性延迟；
e) 智能家居网关设备应支持对控制设备的账户注册、管理、修改、绑定、非法接入报警等功能。

5.3.3 应用程序安装

应用程序安装要求包括：

a) 系统在应用安装时需要获得用户授权，未授权或被用户拒绝的应用，系统应拒绝安装；
b) 若系统支持对未经认证签名的软件下载和安装，在进行应用软件安装前应能对应用软件的签名进行验证；
c) 若系统采用认证签名机制，未经过认证签名的应用软件仅当用户进行确认后才能执行下一步操作；
d) 应用安装时，权限分配采取授权最小化原则，系统应能禁止所有未被允许权限的使用。

5.3.4 应用程序启动

应能防止未经授权或认证的的应用软件启动。

5.3.5 防火墙抗逃逸

操作系统内置的防火墙功能应该具有抗逃逸能力，能够抵抗常见的攻击手段，避免过滤规则被绕过。

5.3.6 安全日志记录及审计控制

安全日志记录及审计控制要求包括但不限于：

a) 宜具备记录用户对设备操作的能力，记录包括但不限于以下内容：用户对设备操作时所使用的

帐号、操作时间、操作内容以及操作结果等；

b) 设备在异常关机、重启、文件系统损坏时产生的告警信息宜自动记入日志；

c) 对于具备文件系统的系统，应具备按帐号分配日志文件读取的能力，防止日志文件被非法读取。仅允许管理员帐号对日志文件进行删除操作；

d) 审计日志应具有循环机制，避免因为日志满而遗漏新事件记录。

5.3.7 安全更新机制

操作系统应具备更新机制，且更新前应得到用户确认，要求包括但不限于：

a) 系统更新时，应对更新文件的来源和完整性进行校验，并应具有原始数据备份能力，能够进行必要的回滚操作，避免更新失败导致系统失效；

b) 系统更新失败时，应保证系统的可用性并给予用户相应的提示；

c) 系统应具备通过补丁或软件升级的方式消除高危及以上等级安全漏洞的能力。

5.3.8 安全防护能力

安全防护能力包括但不限于：

a) 宜支持对病毒、木马的查杀，拦截恶意软件的攻击；

b) 应支持对系统漏洞的修复；

c) 应支持系统补丁的升级。

5.4 应用层安全能力

5.4.1 应用软件签名认证机制

应用软件签名认证机制要求包括但不限于：

a) 支持对未经认证签名的应用软件下载和运行的智能家居终端设备，在进行应用软件安装时应能够识别应用软件的签名状态，并能够根据签名状态给用户相应的提示；

b) 如果智能家居终端设备所下载和运行的应用软件采用认证签名机制，在此情况下，未经过认证签名的应用软件仅当用户进行确认后才能执行下一步操作。

5.4.2 预置应用软件安全要求

预装应用软件不应存在后门等隐藏接口，不应存在高危已知漏洞，不应含有非授权收集或泄露用户信息、非法数据外传等恶意行为。

5.5 外围接口安全能力

5.5.1Web 界面安全

Web 界面安全要求包括但不限于：

a) 应采用安全传输协议，保证 web 访问传输安全；
b) 设备外围接口所提供的 eb 界面不应存在已知高危漏洞，应具备防止绕过攻击能力，导致未经授权的访问。

5.5.2 身份鉴别

身份鉴别要求包括但不限于：

a) 应提供专用的登录控制模块对登录用户进行身份标识和鉴别；
b) 应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；
c) 应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；
d) 应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数；
e) 应支持对异常登录行为的审计功能。

5.5.3 访问控制

应实现用户权限最小化管理，使用分权原则，避免发生权限被滥用等现象的发生。

5.5.4 端口安全

端口安全要求包括但不限于：

a) 不应存在未经声明的外围端口。
b) 设备网络端口不应泄露敏感 Banner 信息，防止攻击者获取后降低攻击难度。

5.6 无线通信安全能力

5.6.1 协议一致性

所采用 WLAN、蓝牙、ZigBee 等无线通信协议应支持设备授权认证、加密传输等安全扩展功能，协议安全相关部分应正确实现与国家相关标准一致。

5.6.2 协议健壮性

应具备非法报文处理能力，当接收到非法报文时应能够正确处理，防止非预期的异常情况发生。

5.6.3 传输保密性

传输保密性要求包括但不限于：

a) 智能家居网关、控制设备与服务端三者之间通信配对时应对密钥进行加密传输，防止密钥泄露；
b) 所采用安全协议，应符合国家相关标准规范，不能使用已被证实安全风险较高的安全协议，如WEP 等；
c) 应支持安全传输通道功能，相关传输加密功能应默认开启。

5.7 用户数据保护安全能力

用户数据保护安全能力包括但不限于：

a) 智能家居终端设备对用户数据中用户个人信息的收集通常应在提供相应服务的同时进行。若出于业务需要而必须事先收集相关数据，应向用户明示事先收集的目的和范围，并且只有在用户同意的情况下方可继续。应向用户提供关闭数据采集功能，在执行此类操作前，应首先对用户身份进行认证；
b) 智能家居终端设备在将位置、健康等用户个人信息存储在终端内部时，应为保存用户个人信息的文件设置适当的权限，以防止未授权的访问。存储生物特征等用户敏感个人信息时，应采用加密形式保存；
c) 智能家居终端设备只有在提供基于位置的服务、通信视频或其它合理的服务场景，且相关服务的有效实现需要联网支撑的情况下，才可通过网络将相关数据转移至终端外部。数据的转移应按需进行，若服务的目的已达成，则应立即停止转移；
d) 智能家居终端设备若通过公共网络传输用户数据，应对数据进行加密，确保信息在网络传输过程中的安全；
e) 智能家居终端设备不应有未向用户明示且未经用户同意，擅自修改用户个人信息的行为。若将用户个人信息存储在终端内部，智能家居终端设备应提供相应选项，允许用户修改或彻底删除已存储的用户个人信息。

5.8 能耗保护安全能力

应具备抗能耗攻击能力，避免由于恶意的能耗攻击，而导致终端电池快速耗尽，而功能失效。

附录 A

智能家居应用设备常见使用场景

（资料性附录）

智能家居应用设备常见使用场景见表 A.1。

表 A.1 智能家居应用设备常见使用场景

分类	描述
安防	入侵报警、火灾监控、水电气监控、可视对话
娱乐	电视、游戏、音乐媒体
视频	视频监控、录像
通讯	呼救设备、多媒体通讯设备
计量	远程抄表、能耗提醒
监测	温度、湿度、光照度等环境监测
生活	微波炉、空调、电冰箱、洗衣机等

电信终端产业协会团体标准

智能家居终端设备 通用安全能力技术要求

T/TAF 071.1—2020

*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn